INSTALL AND CONFIGURE ACTIVE DIRECTORY DOMAIN SERVICES

INTRODUCTION

This document provides a step-by-step walkthrough for installing and configuring Active Directory Domain Services (AD DS) on Windows Server 2022. It covers essential tasks such as promoting a server to a domain controller, setting up DNS, creating a forest and domain structure, and managing users, groups, and organizational units. Additionally, it explores administrative tools and best practices related to delegation, fault tolerance, and FSMO roles. The goal is to establish a secure and manageable domain environment suitable for enterprise operations.

To perform this laboratory, a new virtual machine with Windows Server 2022 has been installed.

INSTALLATION OF ACTIVE DIRECTORY DOMAIN SERVICES

Previously, only two things have been done:

1. Change the name of the machine.
2. From NAT to bridge mode so the VM can communicate with other devices in the network.

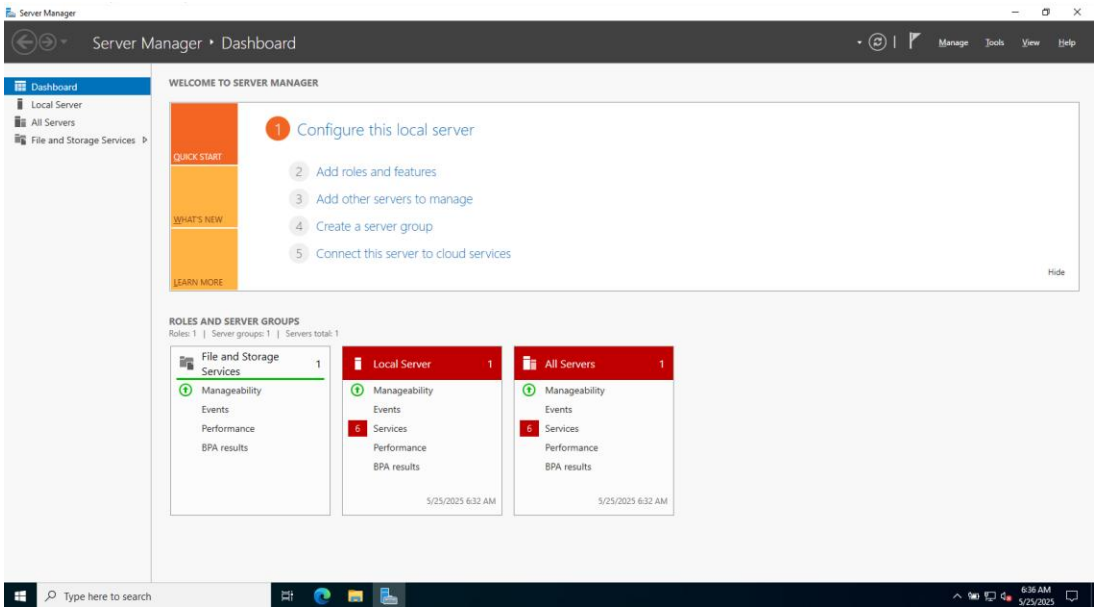
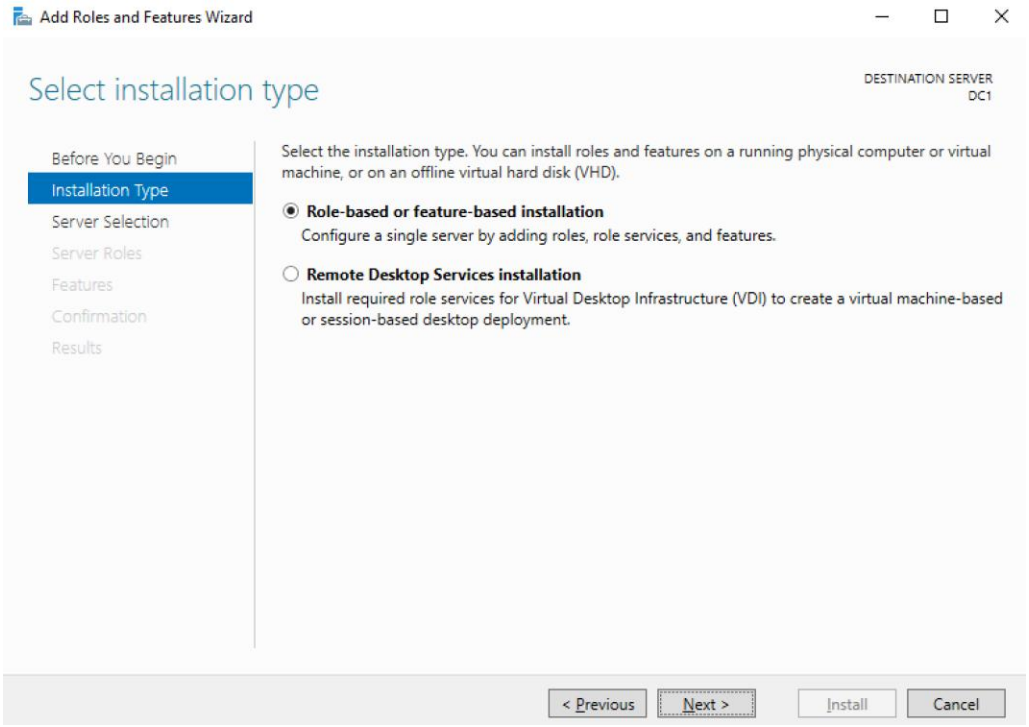


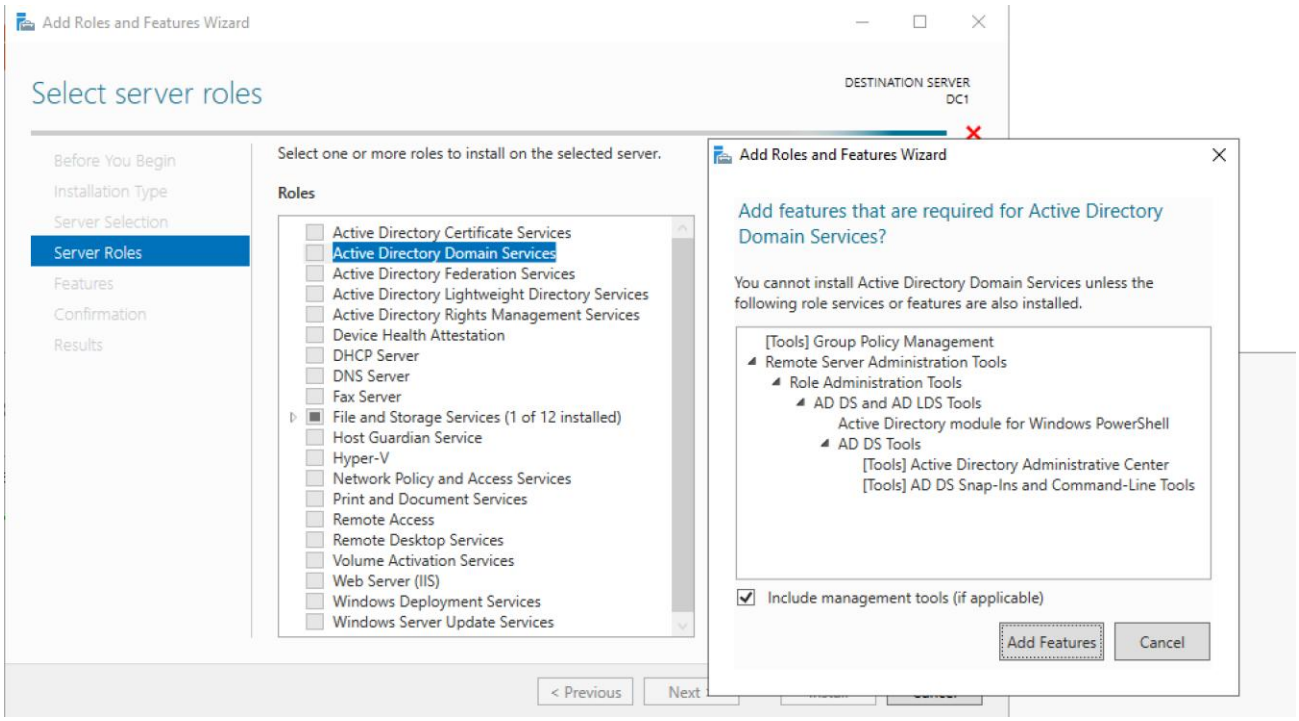
Image of the Windows server with no configuration

To start configuring the machine click on “Add roles and features”. Then a new window will pop up.

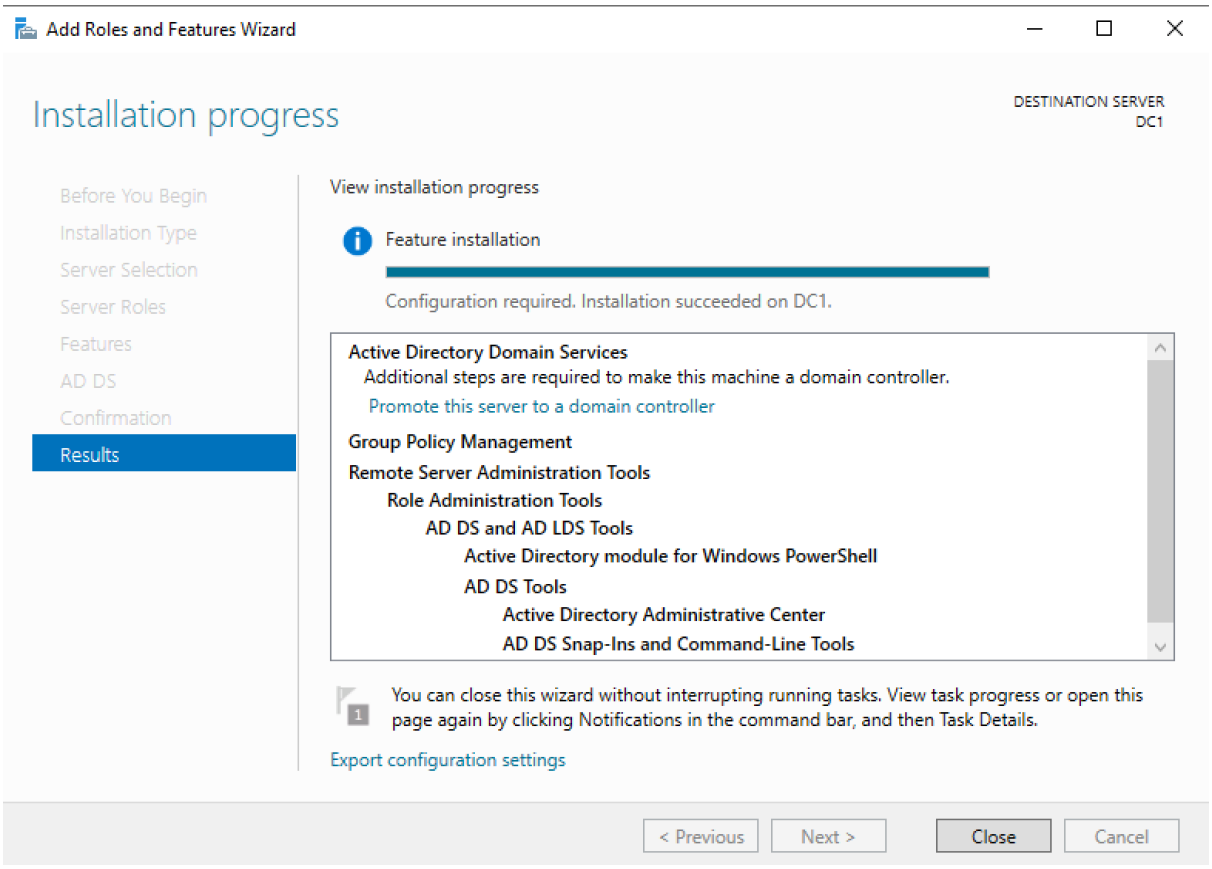


This new window has 7 “steps” to go through.

- Before you begin: The first step is just a bunch of things the administrator must have in mind when installing new features. Click on Next.
- Installation type: Select Role-based or feature-based installation. Click on Next.
- Server Selection: Choose what server this role is going to be installed on. Select the server, then click Next.
    - Note: It is possible to add additional servers that can be managed remotely.
- Select Roles: Choose the specific role or roles to install. In this case, “Active Directory Domain Services” will be selected. Once selected the role a new window will pop up. This new window says that in order to install AD DS more features are required. Click on “Add Features”, and on the main window click on Next.

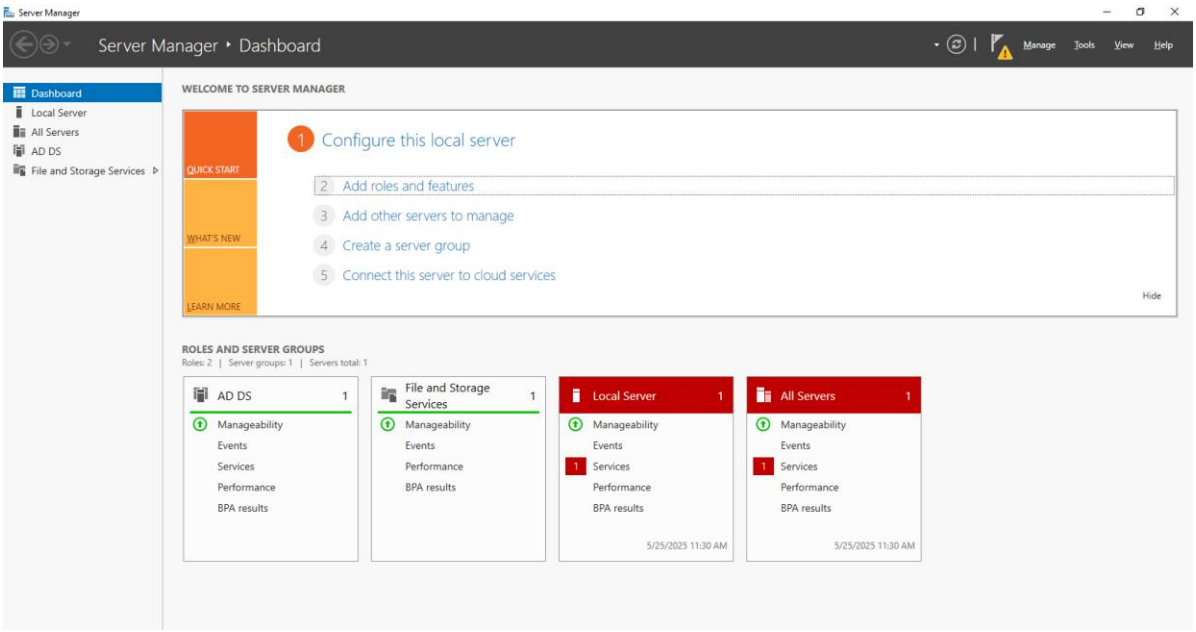


- Features: It is another window where additional features can be added. In this case, no extra features will be added. Click Next.
- Confirmation: It lists all the things that are going to be done. Check the box that says, “Restart the destination server automatically if required”. A warning window will pop up, click on “Yes”. Finally click on “Install.”
- Results: It gives a summary of what was installed. It is important to mention that below the progress bar, there will be a text saying, “Configuration required”. To this point, a new role has been added, however, we must configure it.



Final window of the installation process.

Now, in the sever manager dashboard the AD DS is visible; however, it will be configured as a “Domain Controller”.

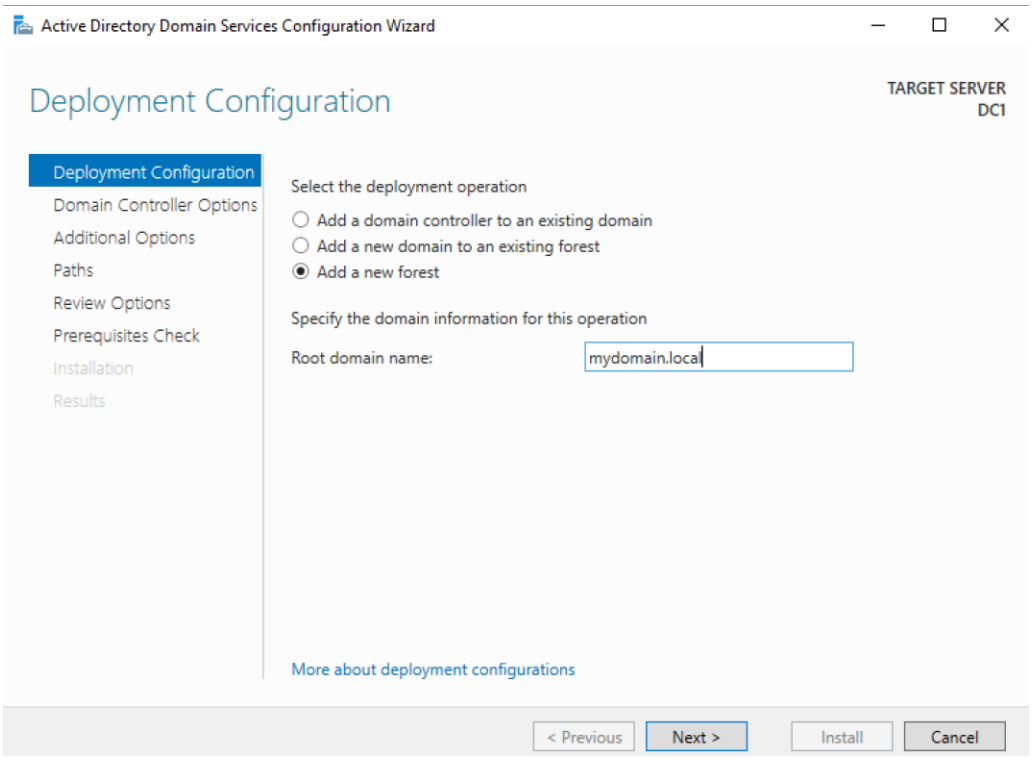


Server Manager Dashboard

DEPLOYMENT CONFIGURATION TYPES FOR AD DS

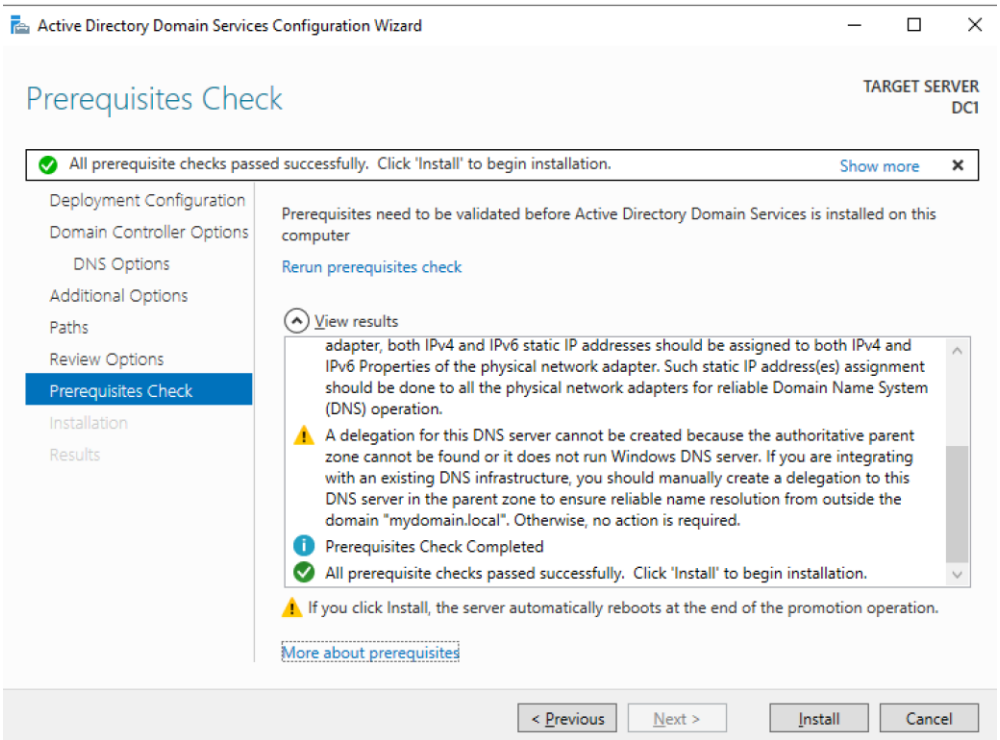
In the last picture, a warning icon at the top left is visible. It indicates that the AD DS need to be configured. Once click on “Promote this server to a Domain Controller”, a new window will pop-up. This window will help to configure the server, and it will take through many steps.

Add a new forest installation.



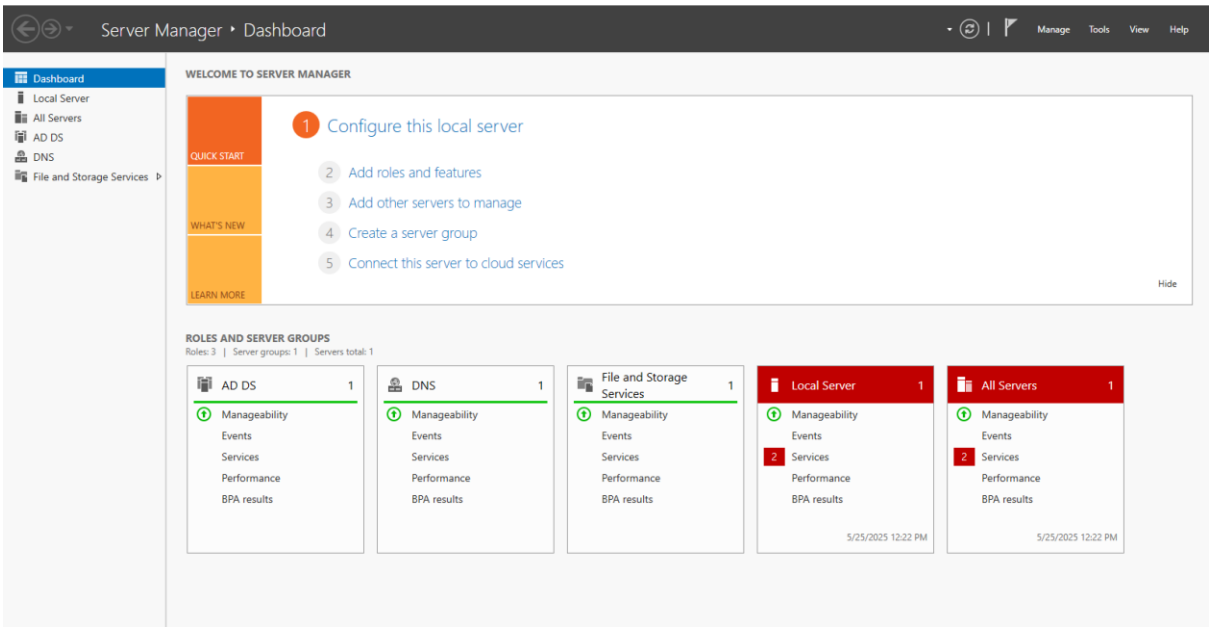
AD DS configuration wizard

- Deployment Configuration: Choose the desired operation. In this case, “Add a new forest” is selected, and a root domain name must be provided. In this case, “mydomain.local” is that name.
- Domain Controller Options: Choose the functional level of the new forest and root domain. In this case, the options are going to stay as they are; additionally, a new password will be configured. Then, click on Next.
    - Note: The idea of “functional level” was discontinued in Windows Server 2016. However, if there are older domain controllers, this functional level has to match with every older domain controller so they can communicate properly.
    - It is a clever idea to have one of the domain controllers also be a DNS server.
    - At least one “Global Catalogue” must exist in every forest.
- DNS options: This window will warn that the DNS could not be found. This is true since we are creating this new Domain Controller with DNS capabilities. Therefore, this warning can be ignored. Click on Next.
- Additional Options: It will suggest a name; it will be taken, and click on Next.
- Paths: This window will ask for the paths of the database, logs, and sysvol. In this case, it stays as it is and click on next.
    - Note: In production environments, it is a clever idea to put each one of them on its storage drive.
- Review Options: It shows a review of all the changes that are going to be applied. Click on Next.
- Prerequisite check: This window will check that the machine has everything it needs to install the rest of AD DS and become a domain controller. Despite having some warnings, a green check appears. Click on Install.



Configuration of the AD DS to become a Domain Controller

The installation involved rebooting the system. After a few seconds, the AD DS and the DNS will be ready to operate.



Server Manager Dashboard

Once the installation is completed, another domain controller is needed in the environment. It is always a clever idea to have some degree of fault tolerance and redundancy in the environment.

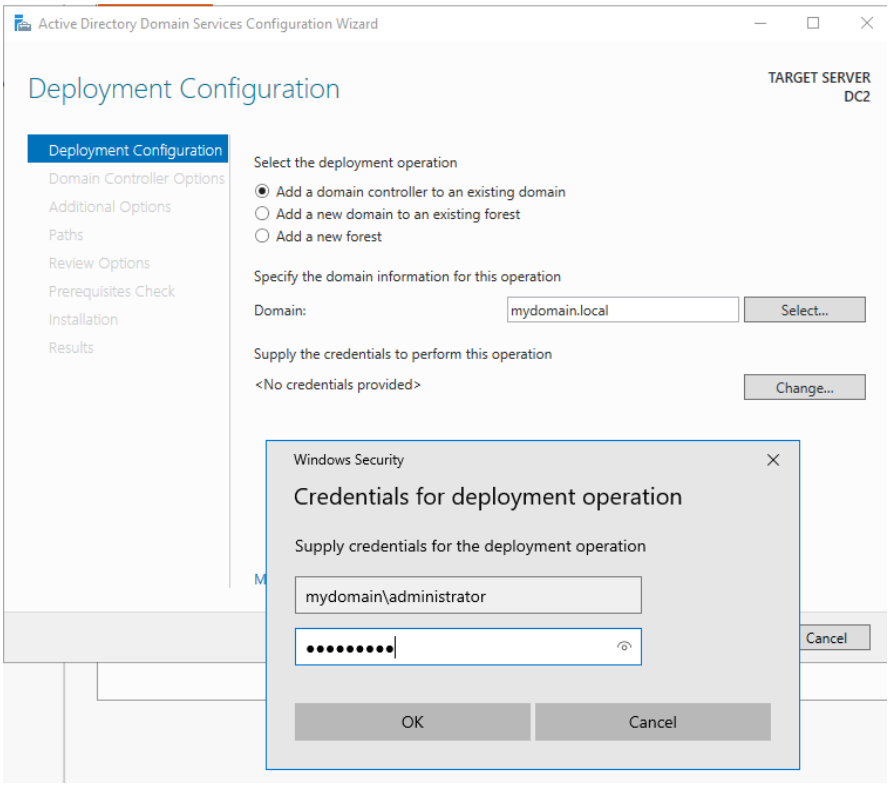
It is important to mention that the second domain controller must have its DNS point to DC1 since DC1 was configured as a DNS server.

The Active Directory Domain Services ser is going to be configured as the previous one. However, some changes must be made when setting up the AD DS.

Add a domain to an existing domain.

This configuration process will mention:

- Deployment Configuration: In this case, the “Add a domain controller to an existing domain” option is going to be selected. Then, the domain name must be typed in the Domain field.
    - Note: The credentials to perform this operation must be provided. Click on Change.



DC2 deployment configuration

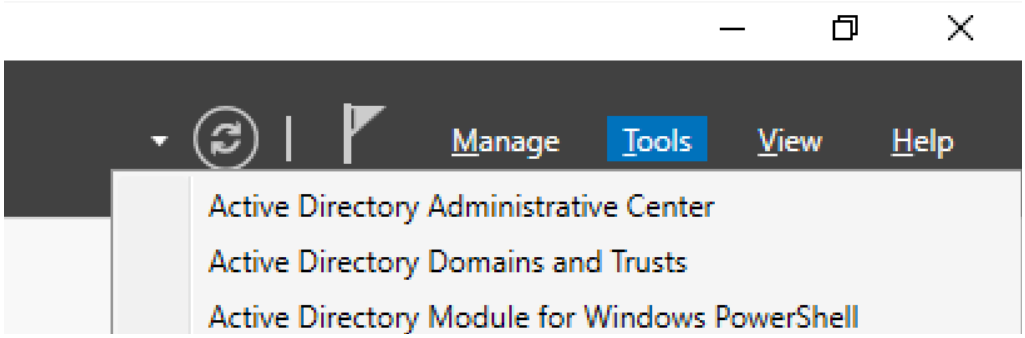
- Domain Controller Options: This window will show some options previously discussed. To have fault tolerance, DNS and Global Catalogue will remain selected. Click on Next.
- DNS Options: Previously mentioned. Click on next.
- Additional Options: Choose where the AD DS' database is going to be replicated. Typically, the replication source is going to be any domain controller. Pick Any domain controller and click on Next.
- Paths: Previously mentioned. Click on Next.
- Review Options: Previously mentioned. Click on Next.
- Prerequisites check: Previously mentioned. Click on Install.

It is important to highlight that there are going to be situations where no IT staff are in an office branch. The option to go is creating a read-only domain controller. Therefore, no changes can be made even if there would be a security breach.

ACTIVE DIRECTORY ADMINISTRATION TOOLS

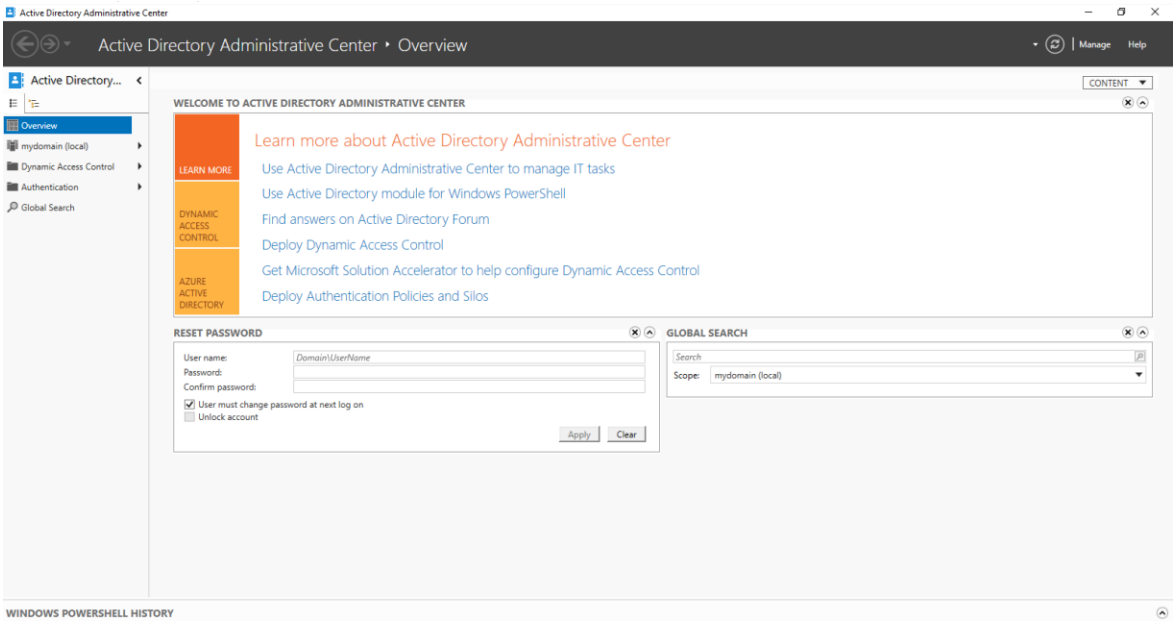
Active Directory Administrative Centre

To enter the Active Directory Administrative Centre, at the top right of the Server Manager Dashboard, click on "Tools" and then "Active Directory Administrative Centre".



Active Directory Administrative Centre

A new window will pop up, that window will look like the image below.

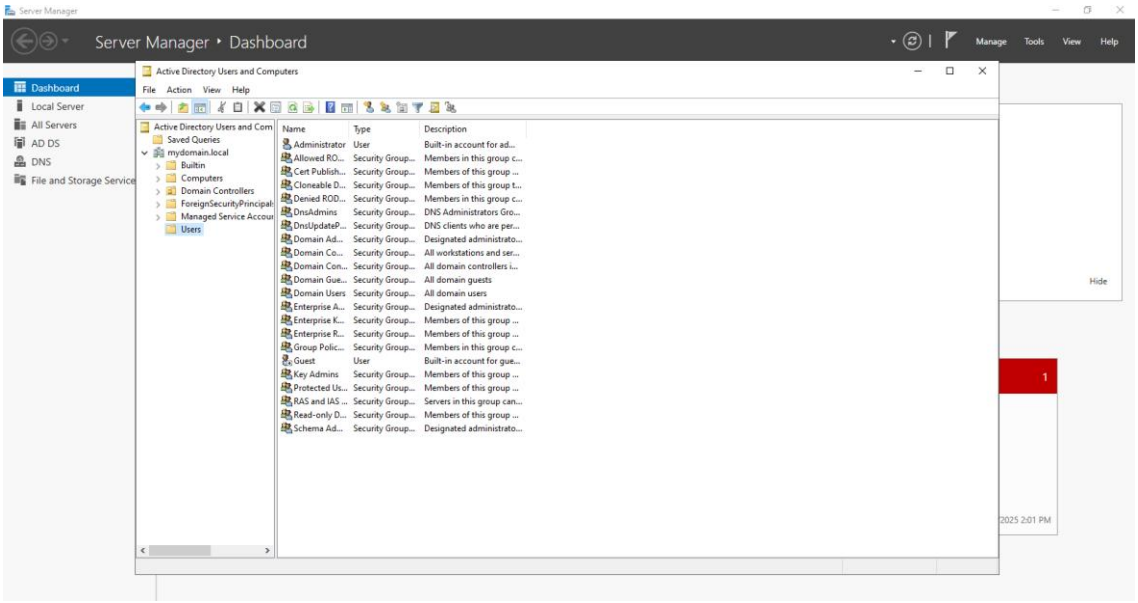


Active Directory Administrative Centre Overview

In this window, tasks related to the active directory will be performed.

Active Directory Users and Computers

One common tool that is going to be used is “Active Directory Users and Computers”. It can be accessed from the tool options. This tool is going to look like the image below:



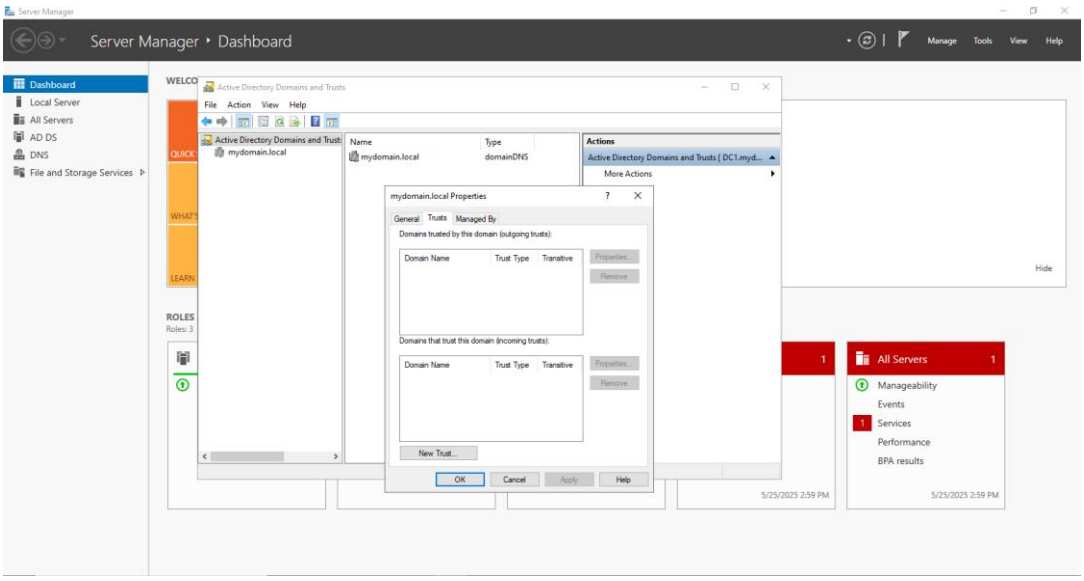
AD users and computers Overview.

It is important to mention that this tool was not built on Power Shell, and even though it is probably the most used tool, it is also the older and more limited tool.

Active Directory Administrative Centre and Active Directory Users and Computers can be used for all the same functions.

Active Directory Domains and Trusts

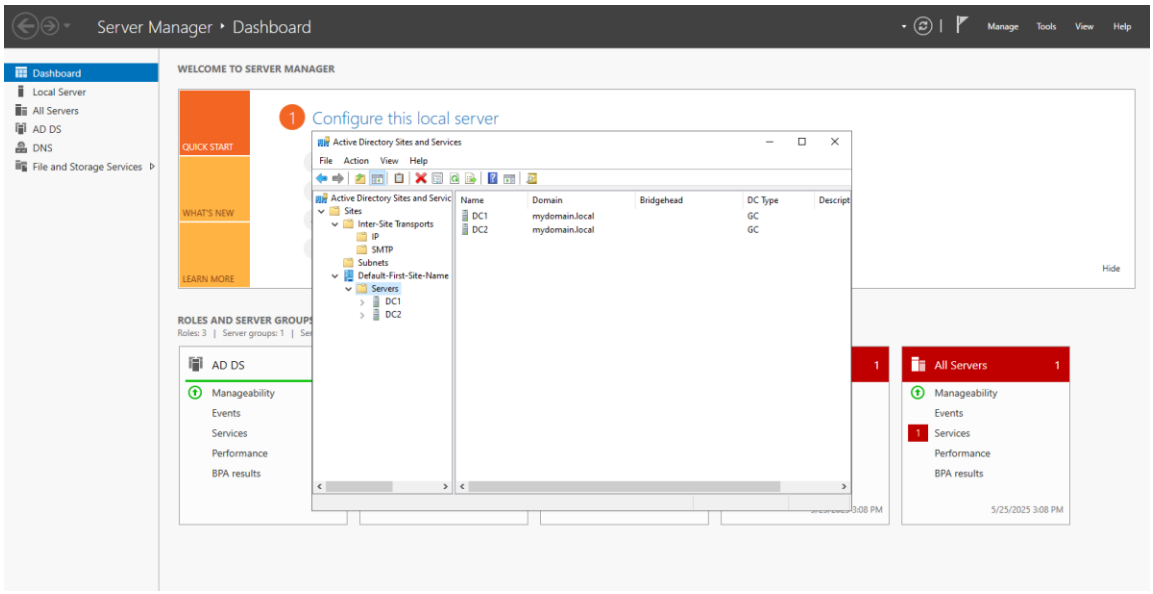
Active Directory Domains and Trusts can be accessed from the Tools option. In this tool is where the hierarchy of different domains an organisation may has. Here, the administrator can manage the trust between those domains.



AD Domains and Trusts Overview

Active Directory Sites and Services

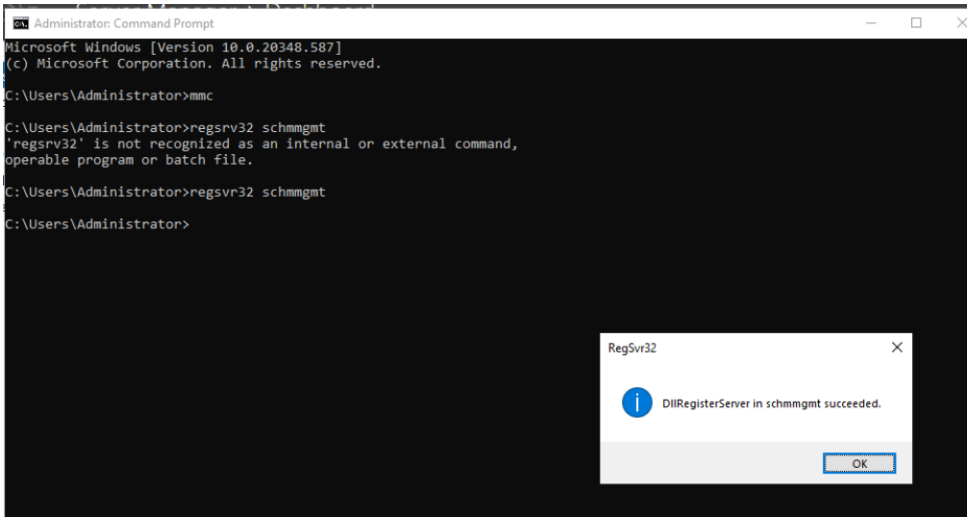
The main functionality of this tool is to manage sites; they are a representation of the different physical locations that an administrator may have in an organization.



AD Sites and Services Overview

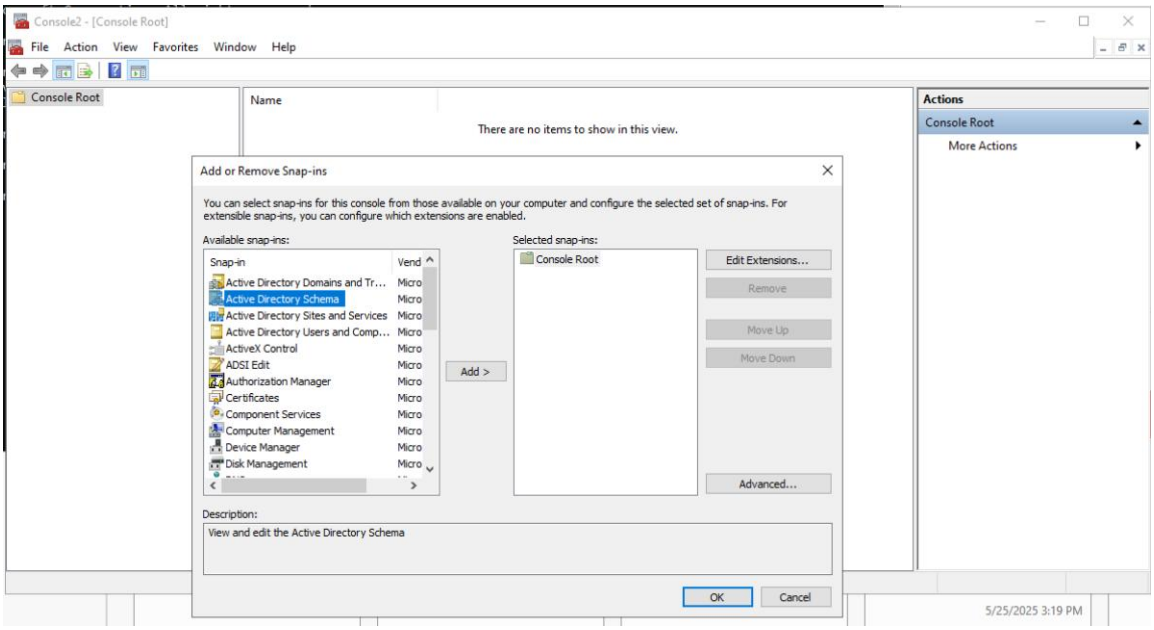
Active Directory Schema

This tool can not be accessed from the Tool menu like the other tools. To access to this tool, the command “regsvr32 schmmgmt” in the CLI as is shown in the image below.



Command to allow the schema tool.

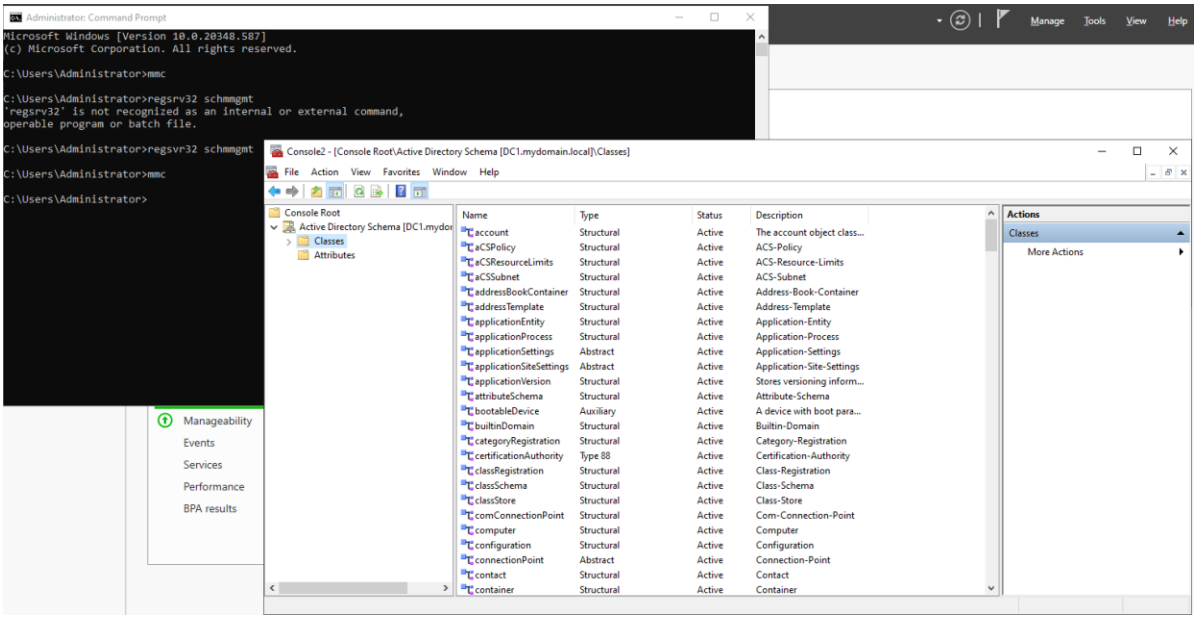
After that, with the command “mmc” the Snap-ins tool will open. This is where the schema tool will be available.



Enabling the AD Schema tool.

Once added and clicked on Ok. The tool will be available.

This tool will contain two folders. The first one is called “Classes,” where there are all the types of objects that exist in Active Directory. The second one is called “Attributes” which is a list of all the different attributes that can be found in all the various objects within Active directory.



AD Schema Overview

FLEXIBLE SINGLE MASTER OPERATIONS - FSMO

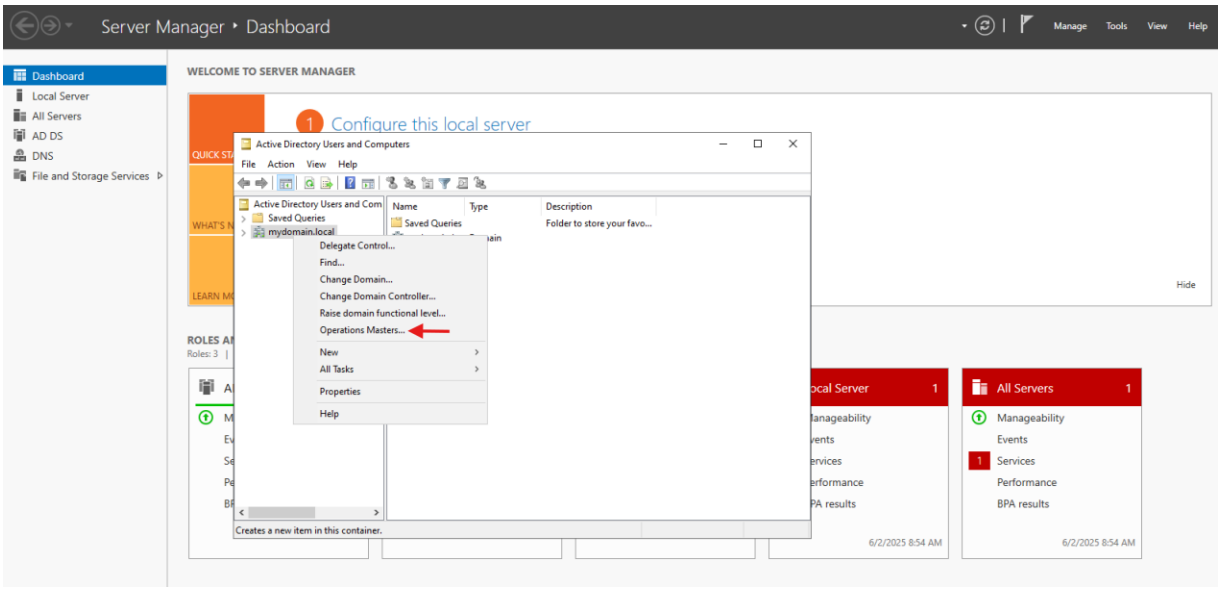
There are 5 FSMO roles in Windows Server 2022.

There are 3 at the domain level (RID Master, PDC Emulator Master, and Infrastructure Master), and two at the forest level (Schema Master and Domain Naming Master).

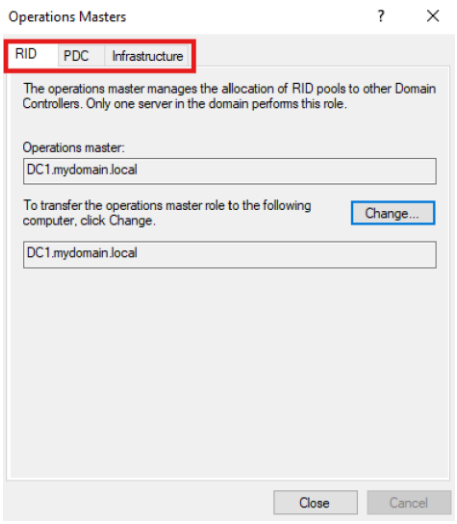
In every domain, there must be one master for every domain. By default, the first domain controller installed in the domain will be the master.

To find roles at the domain level:

- Go to the Tools menu and click on Active Directory Users and Computers.
- Right-click on the domain name and click on Operations masters.



Operations Masters Option



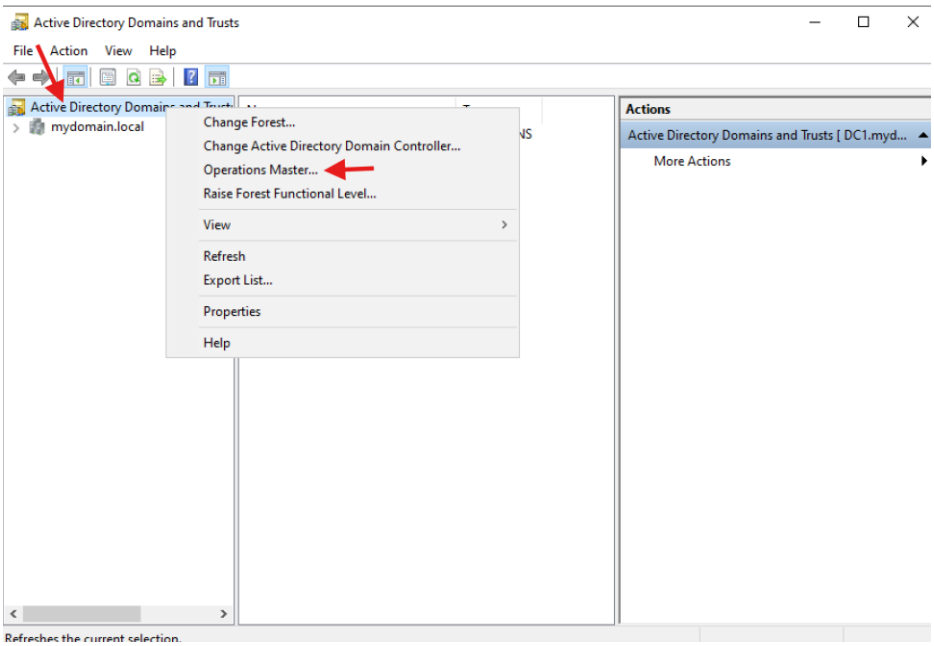
Operations Masters Window

- On the top menu from the operations master window, there are three roles mentioned earlier (RID, PDC, Infrastructure).
    - RID (Relative ID) master: This operation master manages all the allocation of RID pools to other domain controllers. This can be done only for one domain server in the domain.
    - PDC master: This emulates the function of a primary domain controller for pre-Windows 2000 clients. This can be done only for one domain server in the domain.

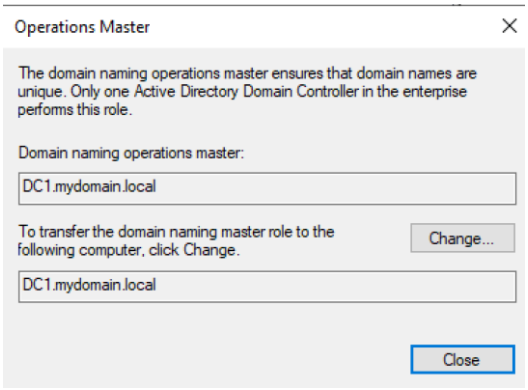
- Infrastructure master: This ensures consistency of objects for inter-domain operations. This can be done only for one domain server in the domain.

To find one role at the forest level:

- Go to the Tools menu and click on Active Directory Domains and Trust.
- Right-click on the Active Directory Domains and Trust object and then click on Operations Master.



Operations Master Option

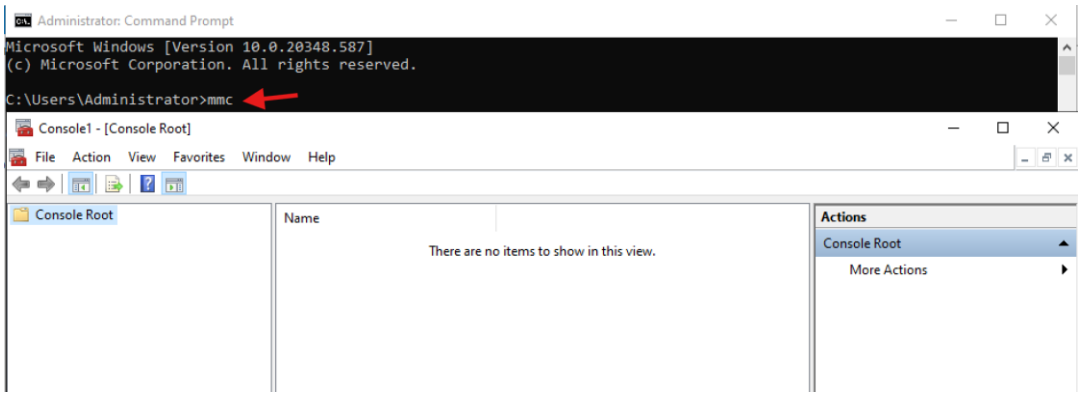


Operations Master Window

- This is the Domain Naming Operations Master, which ensures that the domain names are unique within the forest. This can be done only by one Active Directory Domain in the enterprise.

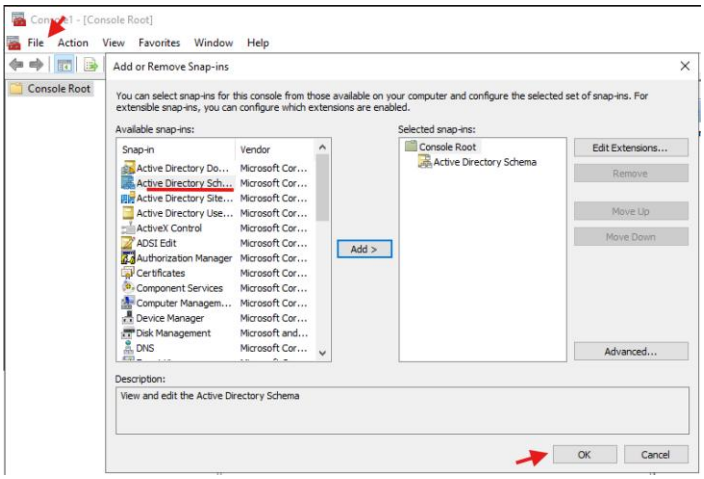
To find the last role:

- Go to the command prompt by searching for cmd on the search bar, then type the command mmc.



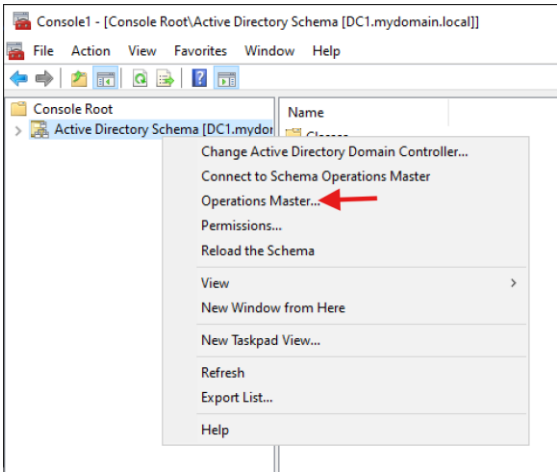
Console Window

- Go to File and click on Add/Remove Snap-in. Then, select Active Directory Schema, click on Add, and finally click on OK.

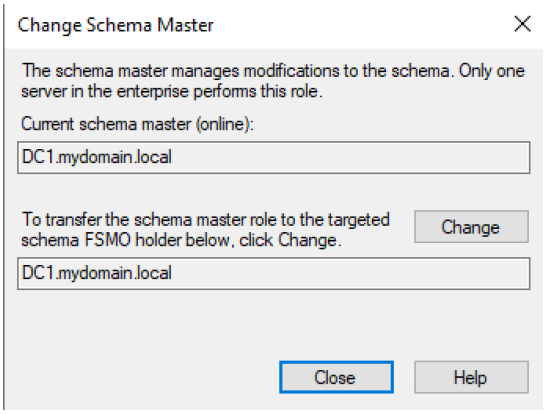


Adding AD Schema to the Console.

- The Active Directory Schema will appear; right-click on it and click on operations master. The Schema master window will pop up.



Operations Master Option.



Schema Master Window

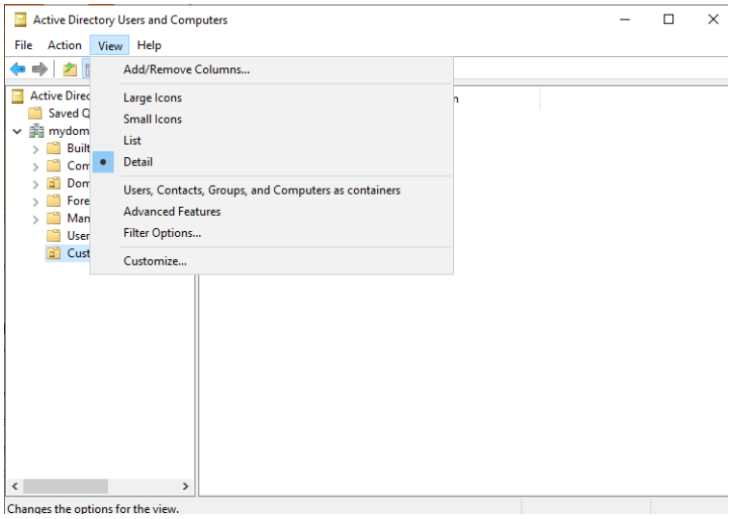
- This schema master manages all the modifications to the schema itself. This will be hosted only for one Domain Controller in the forest.

ACTIVE DIRECTORY PERMISSIONS

Managing the Active Directory environment is one of the most common tasks that an IT professional may perform. In fact, there might be a lot to be done so that the delegation of some of the administrative tasks may be required.

To delegate permissions manually:

- Go to the Tools menu and click on Active Directory Users and Computers. The AD Users and Computers window will pop up.
- To perform the delegation is required to enable the advanced features. To do this, go to View and click on Advanced Features

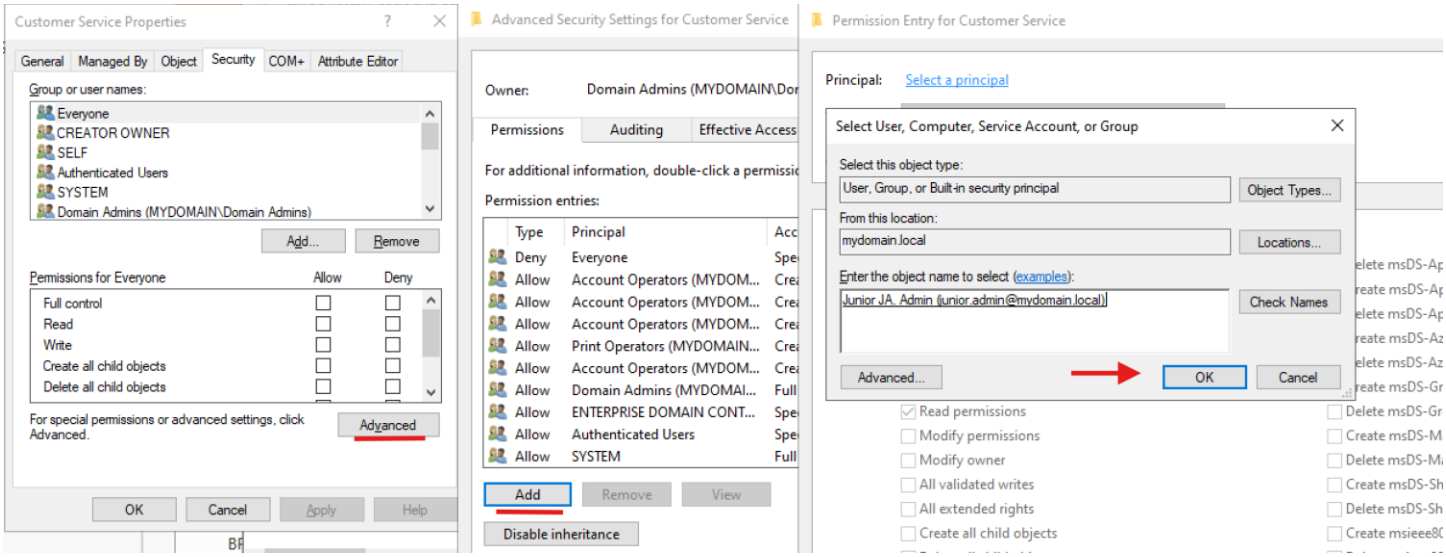


Active Directory Users and Computers window

- Right-click on the organizational unit and then click on Properties. After that, navigate to the Security menu, and there will be the users and the permissions.

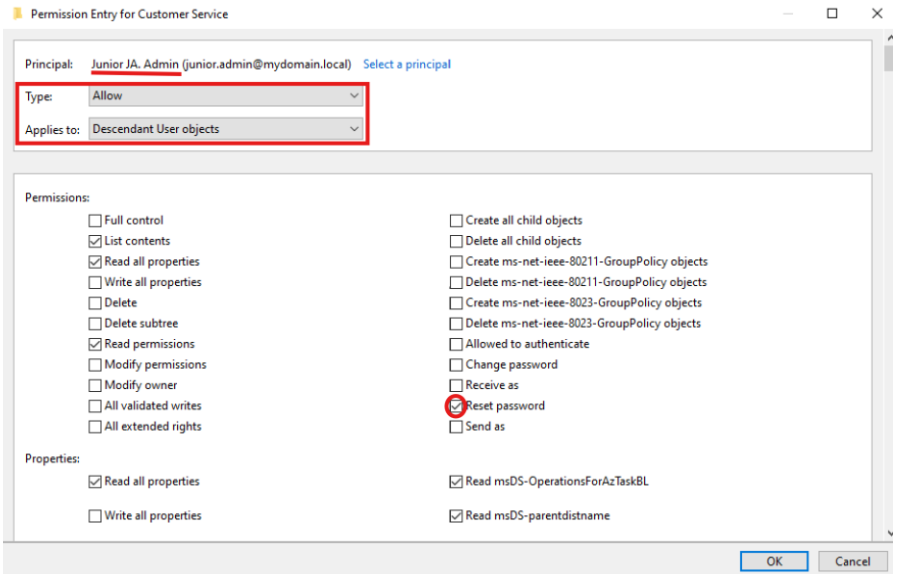
- Note: Whenever giving permissions to users, the least privilege principle must be in mind. This principle says that a user must have only the permissions the user needs to perform his or her job.

- To follow this principle, it is necessary to be granular with the permissions. To do this, click on Advanced, and then click on Add. After that, click on Select a principal, and look for the user that will be granted these new permissions. Finally, click on ok.



Selection of the user.

- Once the user is selected, pick what type of permission is going to be given (Allow or Deny), and to whom this set of permissions applies.
- Select all the permissions that are going to be granted and click on OK.



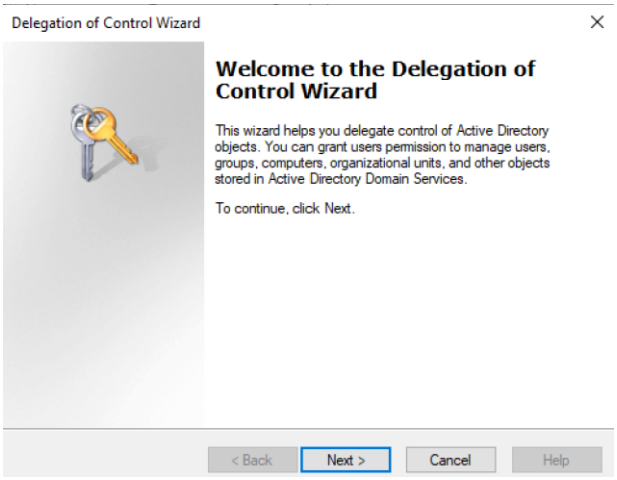
Permission Entry Window

- To finalize the process, click on Ok. Then the user with new permissions will appear on the list of permission entries.

It is important to mention that there is a tool to grant permissions for some of the most common tasks. This tool is called the Delegation of Control Wizard.

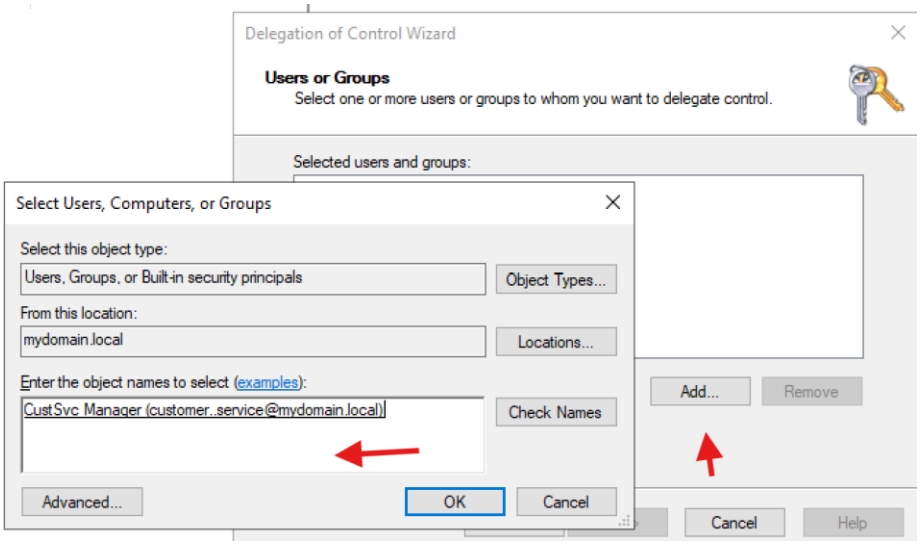
To use this tool:

- The Active Directory Users and Computers window must be open. Right-click on the organizational unit and then click on Delegate Control. A new window will pop up; click on Next.



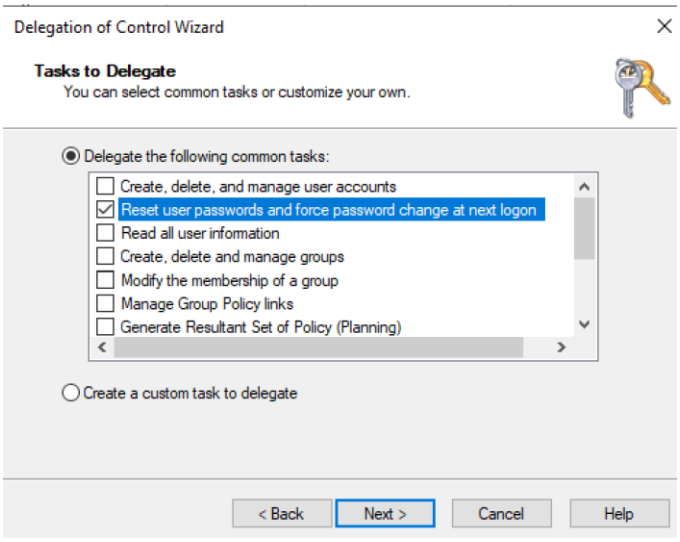
Delegation of Control Wizard Window

- Select the users, computers or groups by clicking on Add, then look for the user that is going to have the new set of permissions. Click on okay, and then click on next.



Select the users' window.

- A new window with the most common tasks to delegate will appear. Select all the tasks needed to delegate and click on Next, then click on Finish.



Delegation Control Wizard

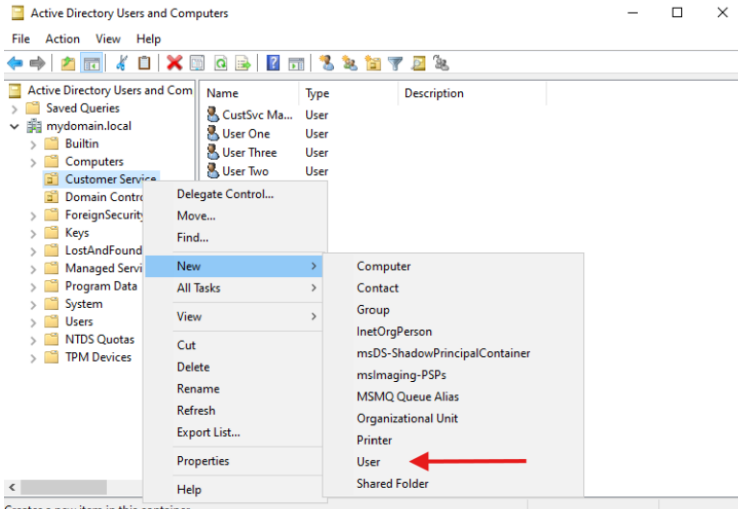
These are the two ways of delegating common tasks to users in the organization.

MANAGING ACTIVE DIRECTORY OBJECTS

There are many different types of objects that can be found in Active Directory; one of the most common objects is the user account object. This object is Active Directory's representation of an actual user on the network. This account is used to assign different rights and permissions to be able to access resources or perform functions on the network.

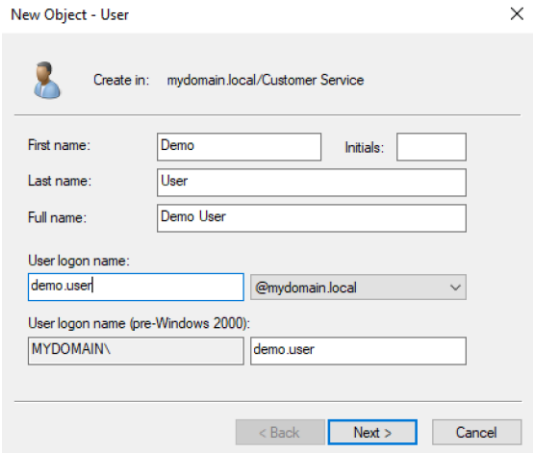
Creation of a user account

- Go to the Tools menu, and click on Active Directory Users and Computers
    - Note: This is the old version that has been around since the early 2000s. Here are displayed many containers (folders); it is not mandatory to create a new user within the Users container.
- Select a container, right click on that container, then hover over New and click on User.



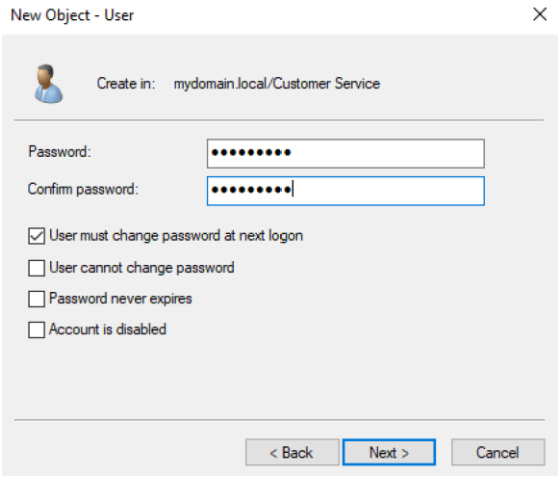
User's creation process.

- The New Object – User window will pop up.
- Fill the boxes with the requested information and click on Next.
    - Note: In the User logon name, it is advisable to use the naming convention that is in place.



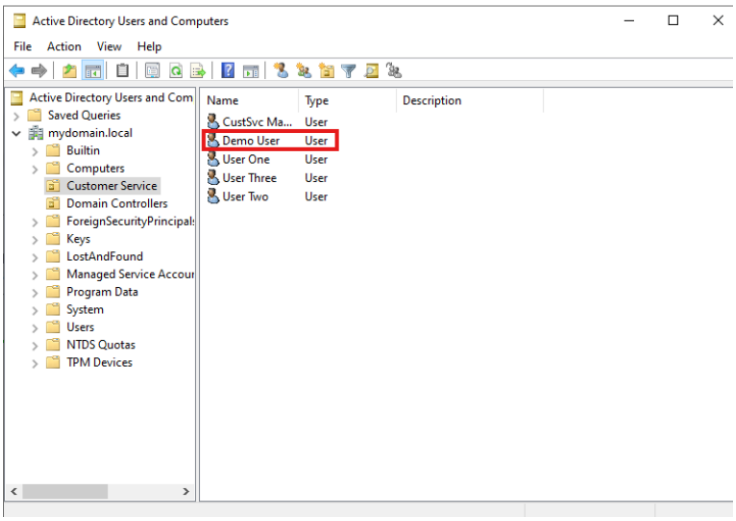
New object window

- Type a password for the user and check the boxes that are needed.
    - Note: User must change password at next logon is a good practice.



New object window

- Finally, click on next and then on finish.



Creation of a new user.

The user was successfully created, and it is visible under the selected container.

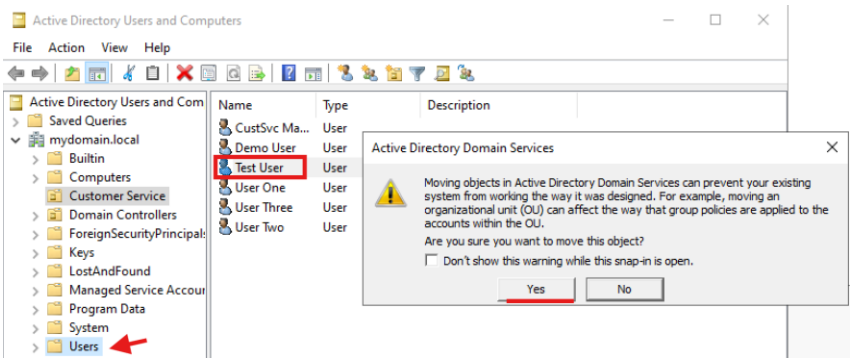
Moving user accounts

When a user exists in a particular container in the Active Directory hierarchy, two things happen to that account.

1. If that account has specific permissions and authority, that authority may change when the user is moved to another container.
2. The group policy settings assigned to a certain container; if a user is moved to another container, those policy settings may also change.

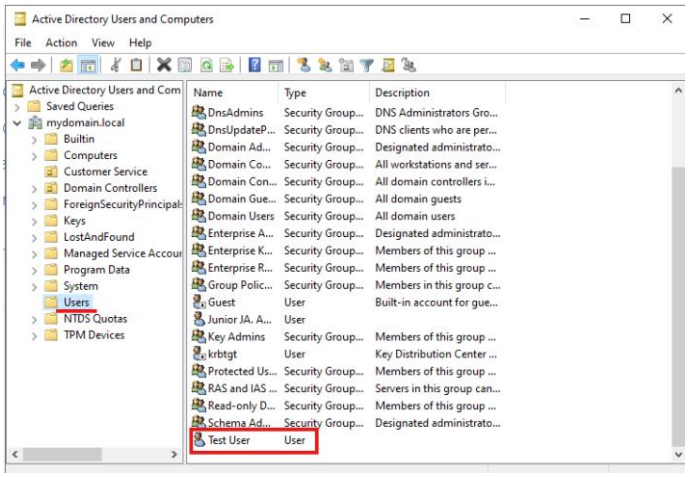
To move a user to another container:

- Go to the Active Directory Users and Computers Tool.
- The easiest way to move the user is to click and drag it to the new container.
    - A warning window will pop up saying the two points previously mentioned.



Moving a user to another container

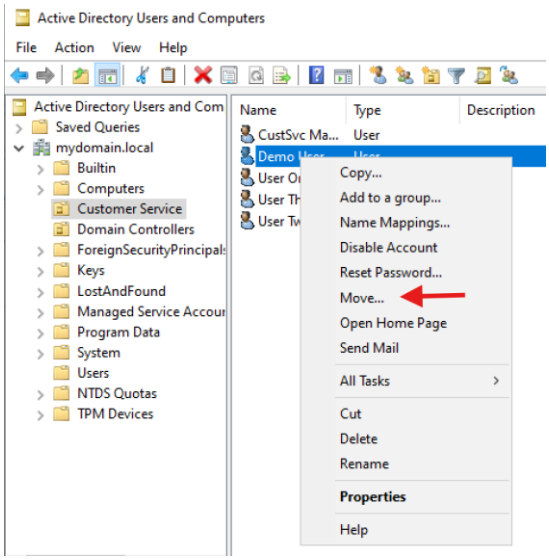
- Click on Yes.
- The user is now moved to the new container.



User under the new container

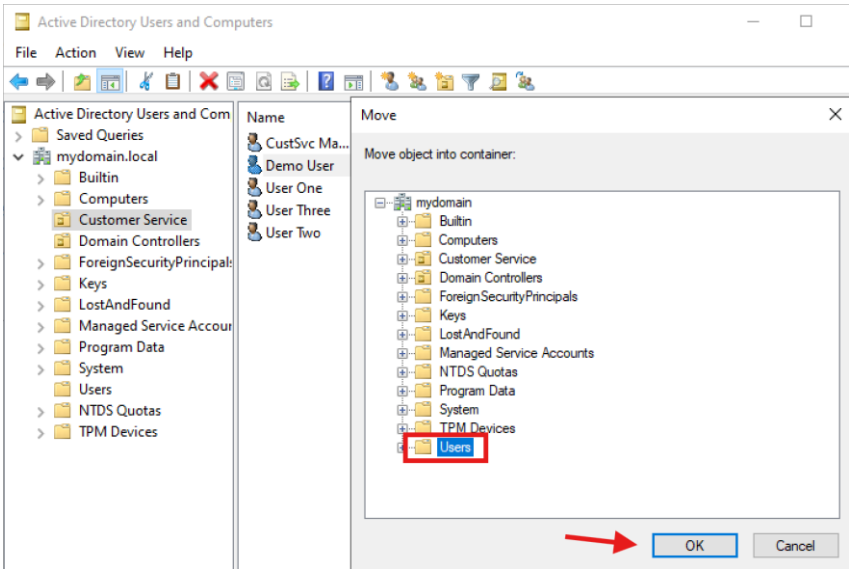
Another option to move the user is:

- Within the Active Directory Users and Computers window. Right-click on the user that is going to be moved, and then click on Move.

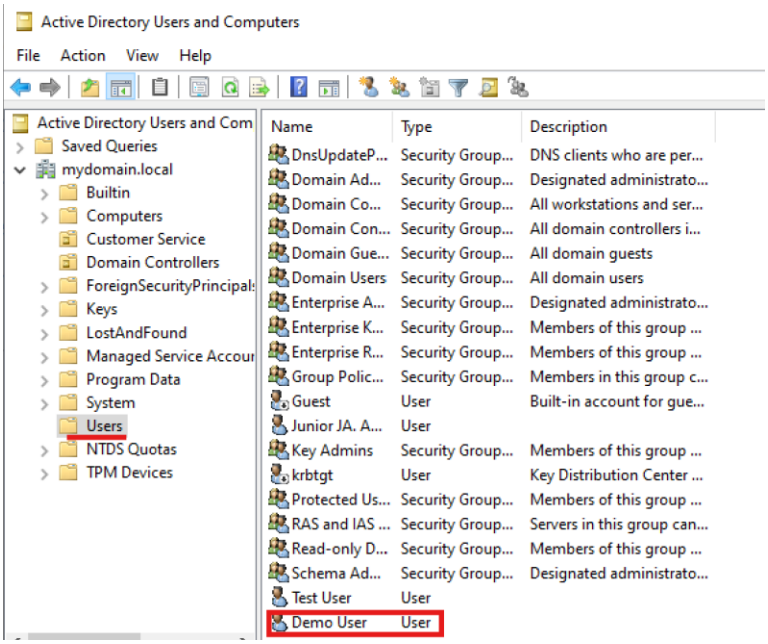


Moving a user to a new container

- A new window will pop up where the new container needs to be selected, then click on OK.



Selecting the new container for a user



User moved to the new container.

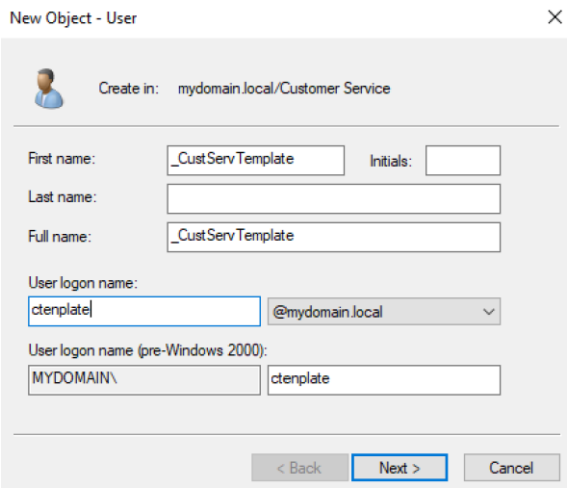
The user was successfully moved to the new container.

User account templates

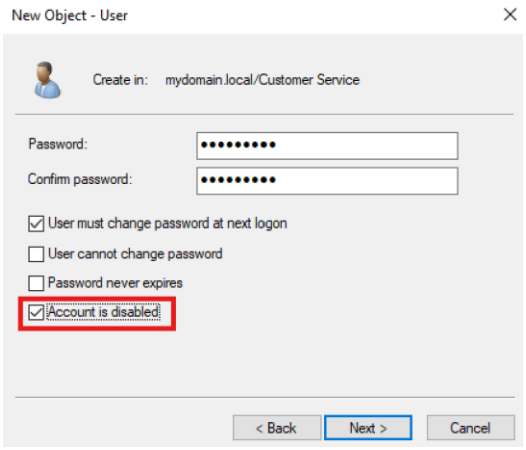
The process of creating user accounts can be repetitive and time-consuming process. A solution to this was the creation of templates; the idea of these templates is based upon the fact that users who work in a similar capacity in an organization are going to have similar needs, and therefore, their accounts could be set up almost identically. This is performed in the Active Directory Users and Computers Tool.

To create a template:

- Create a new user account with a “Template” identifier/label. This identifier should be the name of the account.
- When selecting the options for the account, the option “Account is disabled” must be picked since nobody will use that account to log in to any resource of the organization.

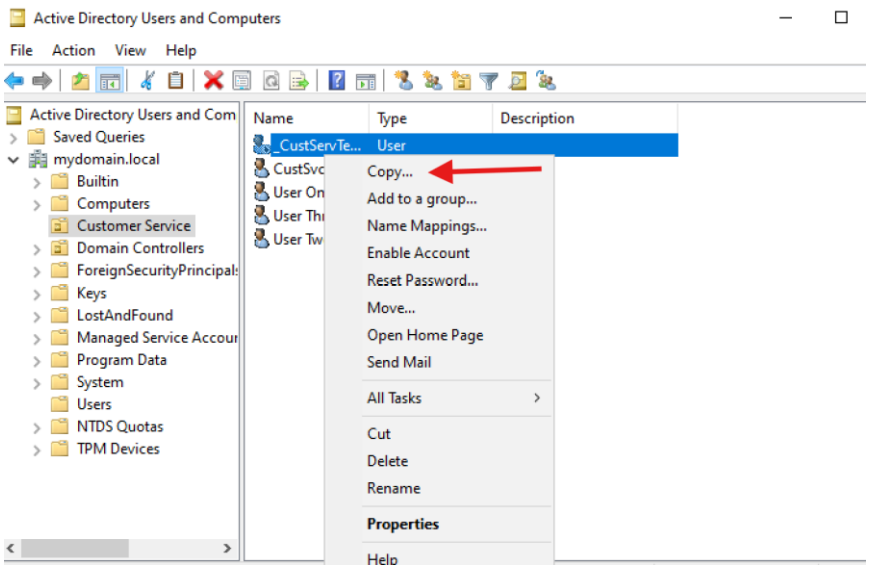


Creation of the template user account

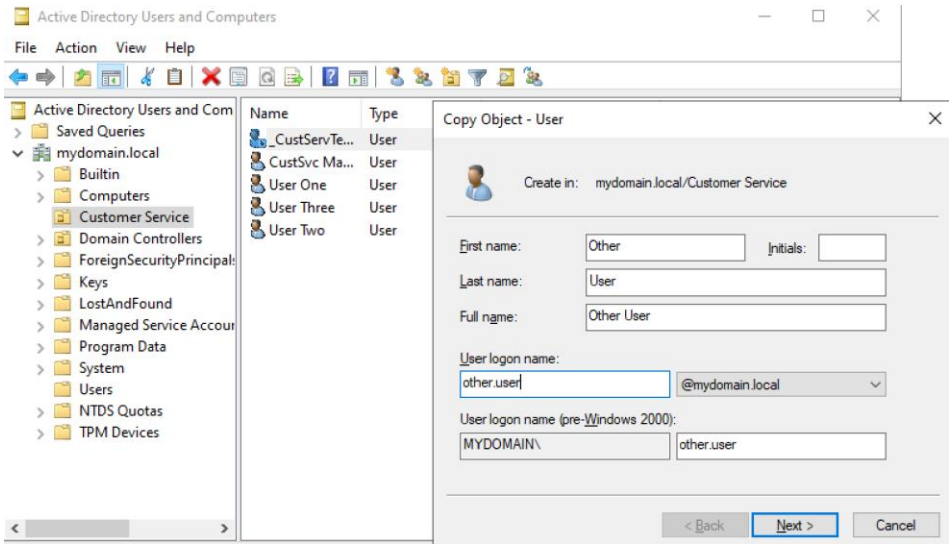


Disabled option checked for the template account.

- Once the template account is created, right-click on that template and click on Copy.
- A Copy Object – User window will pop up. This window is similar to the Create Object window.
- Fill out the required information and click on Next.

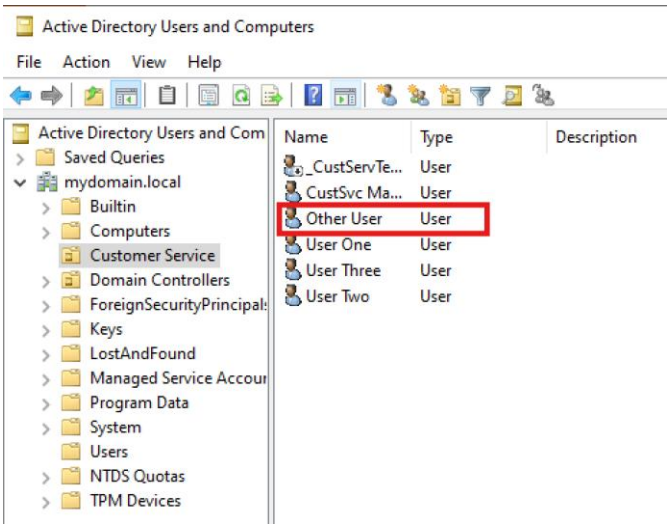


Creation of a new user from the template



Filling out the information to create the user

- Set up a new password and check all the options needed. Click on Next and then Finish.
    - Note: The “Account is disabled” option must be unchecked



New user created from the template.

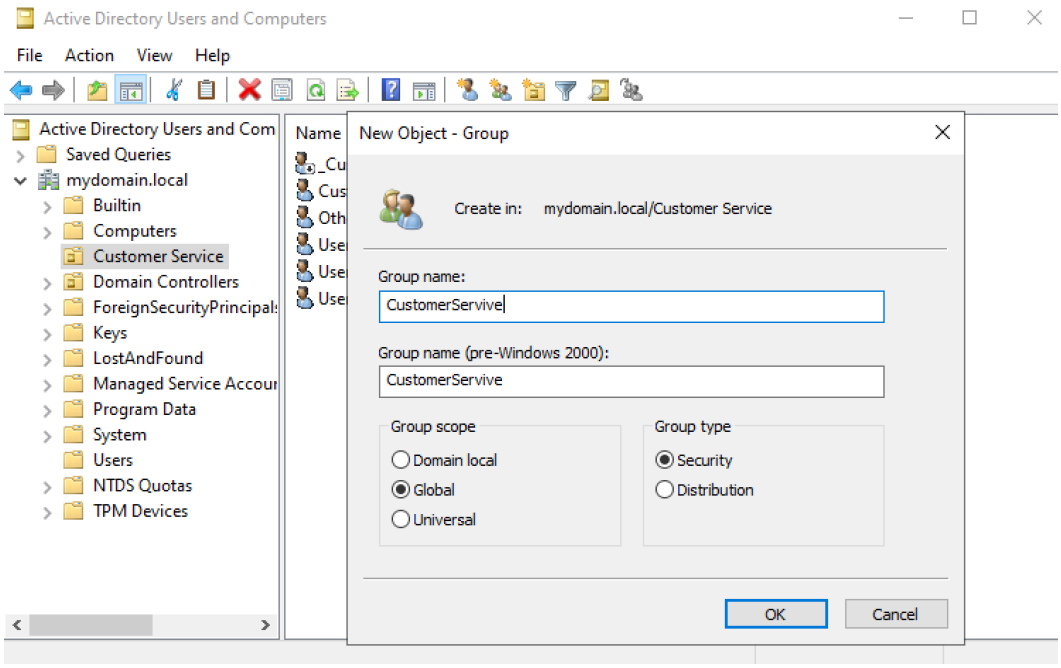
The new user was successfully created from the template. It is important to highlight that even though the configurations are not visible from the Active Directory Users and Computers, the created account will have all the configuration set up on the template account.

Groups on Active Directory

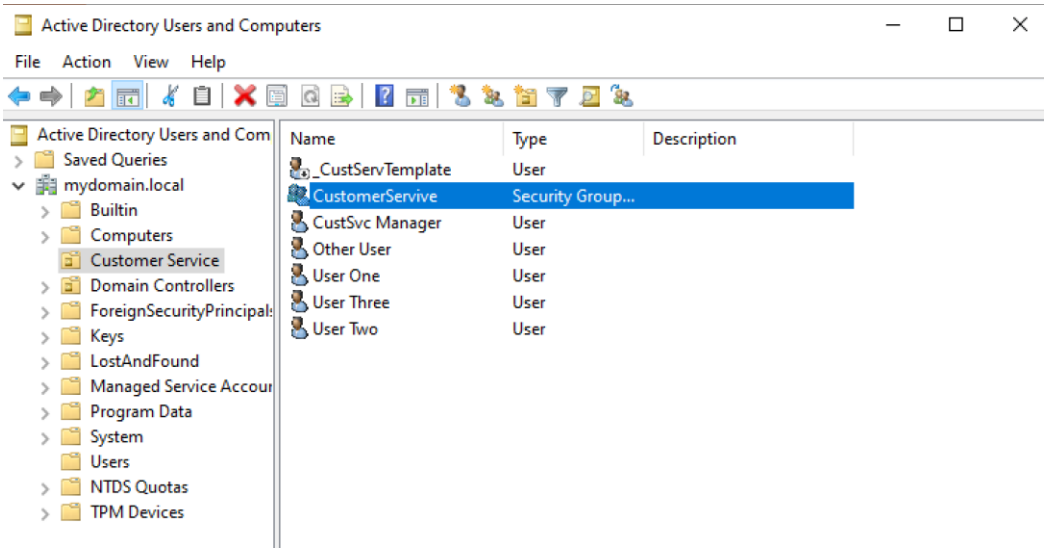
It is recommended that permissions should not be assigned on a user-by-user basis. To achieve this, the use of group account objects within Active Directory is crucial; the idea is that the permissions are assigned to the group, and all the members of that specific group will have the same permissions.

To create a group:

- Go to the Active Directory Users and Computers tool.
- Right-click on the container that is going to have the new group, hover on New, and then click on Group.
- The New Object – Group window will pop up.
- Type a name for the Group and then select the scope and type.
    - There are three different scopes: Domain local, Global (most common), and Universal.
    - There are two different types:
        - Security: It is used to assign rights and permissions to the group
        - Distribution: It is used to send an email to all the members of the distribution group



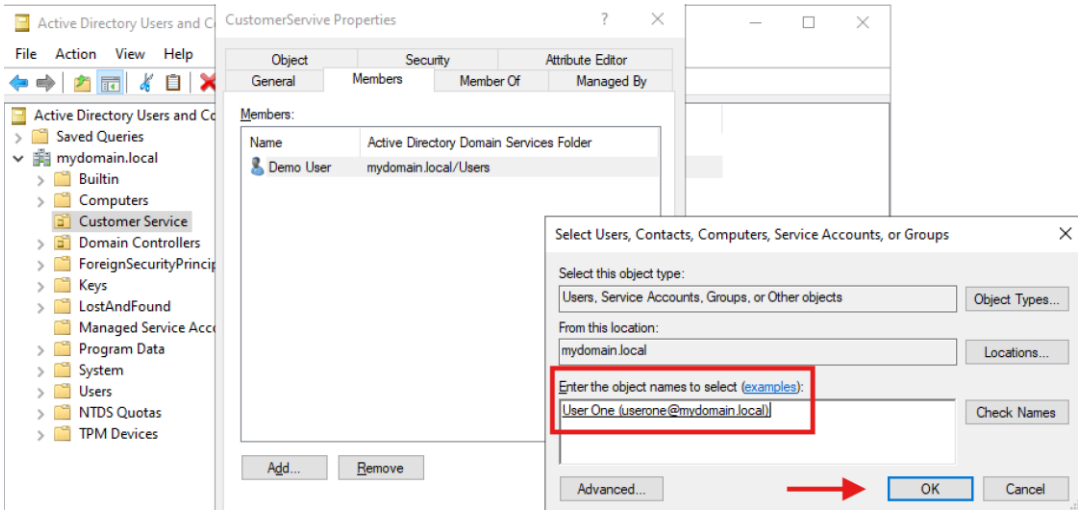
Creation of a Group



The group is visible within the container.

To make users members of a group:

- Within the Active Directory Users and Computers, right-click on the group, and then click on Properties.
- A new window will pop up, click on the Members tab.
    - Note: There is a difference between the Members tab and the Member Of tab. The first refers to adding members to that group, whereas the second refers to being a member of another group. Active Directory allows administrators to have nested groups.
- On the Members tab, look for the users that are going to be part of that group and click Ok.
- After that, the selected user will be part of the desired group.



Adding members to the group

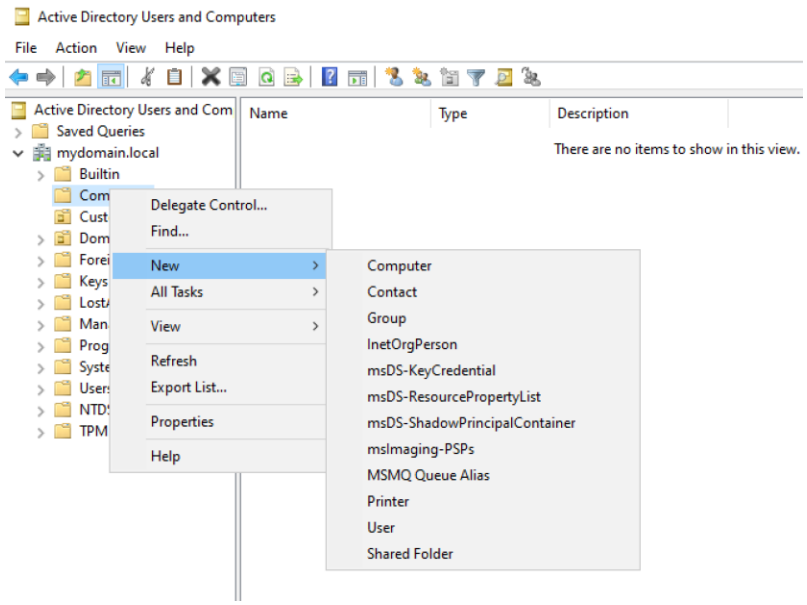
Computer Accounts on Active Directory

It is also a "security principle," but it is possible to assign rights and permissions.

The active directory hierarchy contains a "computer" container, which contains all the computers that have joined the domain.

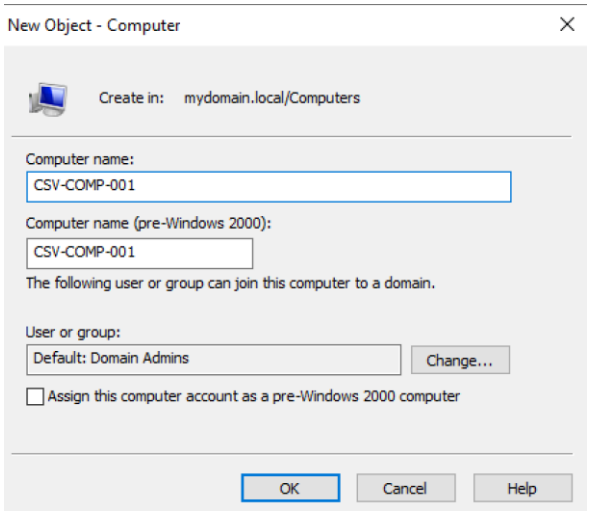
To create a computer account:

- Within the Active Directory Users and Computers, right-click on the Computers container, hover over New and click on Computer. A new window will pop up.



Creation of the Computer object

- A name must be provided for the computer, and click on Ok. After that, the computer account will be created.



Creation of the CSV-COMP-001 computer object

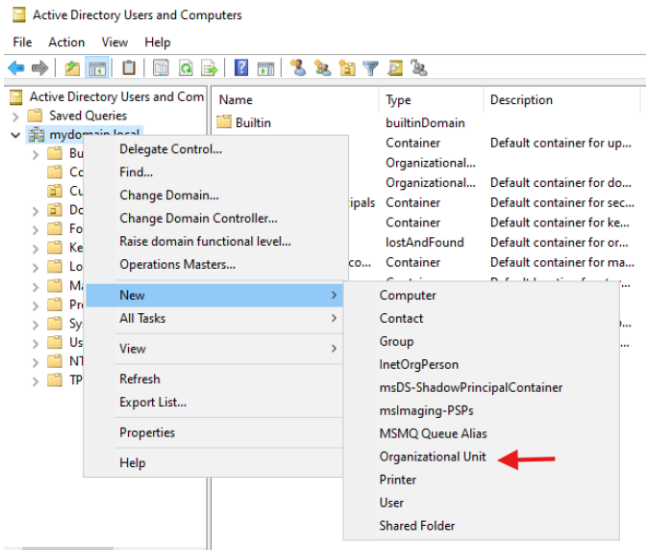
Manually creating a computer object is not done often; this is done when a "pre-stage" of a computer is needed. The reason for pre-staging a computer may be due to specific computers must be added to different containers and not the default container.

Organizational Units (OU)

All the containers that are in the hierarchical structure of the Active Directory are Organizational Units.

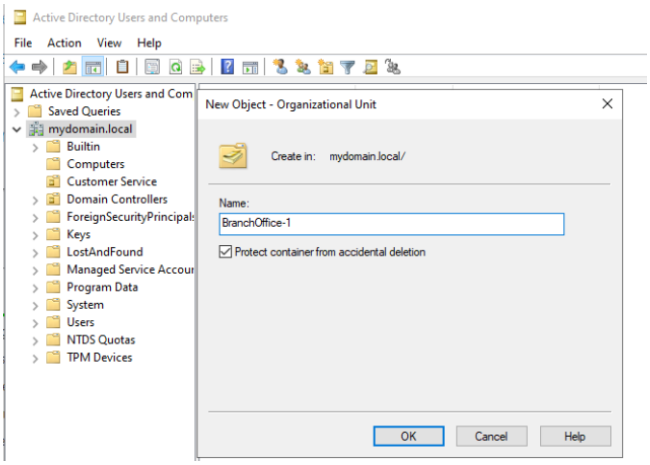
To create organizational units:

- Within the Active Directory Users and Computers, right-click on the domain name, hover over New and then click on Organizational Unit. A new window will pop up.



Creation of an Organizational Unit

- Provide a name to the new organizational unit, the check box for accidental deletion protection could stay cheked, finally, click on Ok.



Creation of the BranchOffice-1 organizational unit

Note: It is recommended by Microsoft that the hierarchy should not go more than 4 levels deep.

CONCLUSION

The successful deployment of Active Directory Domain Services demonstrated a comprehensive understanding of domain controller configuration, DNS integration, and administrative delegation. By implementing redundancy through an additional domain controller and applying best practices like least privilege and proper organizational structure, the environment is now prepared for secure and efficient identity management. The use of AD tools such as Users and Computers, Sites and Services, and the Administrative Centre enabled precise control over users, groups, and computer objects. This setup establishes a reliable foundation for supporting enterprise-scale directory services and ongoing IT operations.